

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

SECURITYPROFILING, LLC,

**Plaintiff/Counterclaim-
Defendant,**

v.

**TREND MICRO AMERICA, INC. and
TREND MICRO INCORPORATED,**

**Defendants/Counterclaim-
Plaintiffs.**

Civil Action No. 3:17-cv-1484-N

**PLAINTIFF'S COMBINED OPENING AND RESPONSIVE
CLAIM CONSTRUCTION BRIEF**

CONTENTS

I.	INTRODUCTION	1
III.	LEGAL STANDARD.....	2
A.	General Rule of Claim Construction	2
B.	Law of Indefiniteness	4
C.	Means-Plus-Function Claiming	6
IV.	DISPUTED TERMS TO BE CONSTRUED	7
A.	“Vulnerability”	7
B.	“Intrusion Prevention System”.....	10
C.	“Firewall”.....	12
D.	“Remediation Technique”	13
E.	“Each mitigation technique has a mitigation type including at least one of a patch, a policy setting, [and/or] a configuration option”	15
F.	“Each remediation technique has a remediation type selected from the group consisting of a patch, a policy setting, and a configuration option”	17
G.	“Occurrence”	18
H.	“Occurrence Packet”.....	21
I.	“Attack”.....	21
V.	CLAIM TERMS DEFENDANT ALLEGES ARE GOVERNED BY 35 U.S.C. § 112(f) 22	
A.	Absence of the noun “means” from the disputed claims creates a presumption that §112(f) does not apply.....	22
B.	Defendants cannot rebut the presumption that § 112(f) does not apply merely by labeling “code” a nonce term synonymous with “means.”.....	28
1.	Claim Terms Concerning Multiple Mitigation Techniques (Claim Terms 10-23). 28	

2. Claim Terms for Updating a Firewall and an Intrusion Prevention System (Claim Terms 24-29).....	31
3. Claim Terms Concerning Identifying an Occurrence in Connection with a Device (Claim Terms 30-31).....	34
4. Claim Terms for Determining Whether Devices Are Actually Vulnerable to an Occurrence or Attack (Claim Terms 32-35)	35
5. Claim Terms Concerning Storing Information Associated with Multiple Actual Vulnerabilities (Claim Terms 36-37).....	36
6. Claim Terms Concerning Data Storage of Device and Vulnerability Information (Claim Terms 38-42).....	37
7. Additional Claim Terms (Claim Terms 43-45)	40
C. In the event the disputed terms are governed by 35 U.S.C. § 112(f), the specification discloses structure sufficient to be understood by one skilled in the art as adequate to perform the functions recited in the claims, rendering the claims definite.	41
VI. CONCLUSION.....	43

AUTHORITIES

Cases

<i>Affymetrix, Inc. v. Hyseq, Inc.</i> , 132 F. Supp. 2d 1212 (N.D. Cal. 2001)	24
<i>Akzo Nobel Coatings, Inc. v. Dow Chem. Co.</i> , 2016 WL 363443 (Fed. Cir. 2016)	4
<i>Aloft Media, LLC v. Adobe Sys. Inc.</i> , 570 F. Supp. 2d 887 (E.D. Tex. 2008), <i>opinion adopted</i> , No. CIV.A. 6:07-CV-355, 2008 WL 5784443 (E.D. Tex. Sept. 24, 2008)	24
<i>Ancora Techs., Inc. v. Apple, Inc.</i> , 744 F.3d 732 (Fed. Cir. 2014)	5
<i>Apex Inc. v. Raritan Computer, Inc.</i> , 325 F.3d 1364 (Fed. Cir. 2003)	23
<i>Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.</i> , 521 F.3d 1328 (Fed. Cir. 2008)...	41, 42,
	43
<i>Atser Research Techs., Inc. v. Raba-Kistner Consultants Inc.</i> , No. SA-07-CA-93-H, 2009 WL 691118 (W.D. Tex. Mar. 2, 2009), <u>aff'd</u> , 384 F. App'x 995 (Fed. Cir. 2010).....	42
<i>Augme Techs., Inc. v. Yahoo! Inc.</i> , 755 F.3d 1326 (Fed. Cir. 2014).....	41, 42
<i>Avid Tech., Inc. v. Harmonic, Inc.</i> , 2016 WL 363410 (Fed. Cir. 2016)	3
<i>Blackboard, Inc. v. Desire2Learn, Inc.</i> , 574 F.3d 1371(Fed. Cir. 2009).....	41, 42, 43
<i>Budde v. Harley-Davidson, Inc.</i> , 250 F.3d 1369 (Fed. Cir. 2001).....	7
<i>Chamberlain Grp., Inc. v. Lear Corp.</i> , 756 F. Supp. 2d 938 (N.D. Ill. 2010).....	25, 42
<i>Cioffi v. Google, Inc.</i> , 2015 WL 7254039 (Fed. Cir. 2015).....	3, 5
<i>Convolve, Inc. v. Dell, Inc.</i> , No. 2:08-CV-244-CE, 2011 WL 31792 (E.D. Tex. Jan. 5, 2011), <i>opinion clarified</i> , No. 2:08-CV-244-CE, 2011 WL 13089002 (E.D. Tex. July 5, 2011)	25
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	5
<i>Enzo Biochem, Inc. v. Applera Corp.</i> , 599 F.3d 1325 (Fed. Cir. 2010).....	5

<i>Eolas Techs., Inc. v. Adobe Sys., Inc.</i> , 810 F. Supp. 2d 795 (E.D. Tex. 2011), <i>opinion withdrawn in part on reconsideration</i> , No. 6:09-CV-446, 2011 WL 11070303 (E.D. Tex. Sept. 23, 2011), and <i>aff'd sub nom. Eolas Techs. Inc. v. Amazon.com, Inc.</i> , 521 F. App'x 928 (Fed. Cir. 2013) 24	
<i>eWinWin, Inc. v. Groupon, Inc.</i> , No. 8:10-CV-2678-T-24, 2011 WL 6012194 (M.D. Fla. Sept. 5, 2011)	42
<i>GE Lighting Sols., LLC v. AgiLight, Inc.</i> , 750 F.3d 1304 (Fed. Cir. 2014).....	4
<i>Greenberg v. Ethicon Endo-Surgery, Inc.</i> , 91 F.3d 1580 (Fed.Cir.1996).....	23
<i>In re Dossel</i> , 115 F.3d 942 (Fed. Cir. 1997)	7
<i>InTouch Technologies, Inc. v. VGO Commc'ns, Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014).....	5
<i>Jurgens v. McKasy</i> , 927 F.2d 1552, 1557 (Fed. Cir. 1991)	6
<i>Kara Tech. Inc. v. Stamps.com Inc.</i> , 582 F.3d 1341 (Fed. Cir. 2009)	3
<i>Kinetic Concepts, Inc. v. Smith & Nephew, Inc.</i> , 688 F.3d 1342 (Fed. Cir. 2012)	6
<i>Lighting World, Inc. v. Birchwood Lighting, Inc.</i> , 382 F.3d 1354 (Fed. Cir. 2004).....	23
<i>Markman v. Westview Instruments, Inc.</i> , 52 F.3d 967 (Fed. Cir. 1995), <u>aff'd</u> , 517 U.S. 370, 388-90 (1996).....	3, 4
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 134 S. Ct. 2120 (2014)	4
<i>Openwave Sys., Inc. v. Apple Inc.</i> , 808 F.3d 509 (Fed. Cir. 2015)	4
<i>Personalized Media Communications, LLC v. International Trade Commission</i> , 161 F.3d 696 (Fed. Cir. 1998).....	22, 26
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (<i>en banc</i>)	3, 4
<i>PPC Broadband, Inc. v. Corning Optical Commc'ns RF, LLC</i> , 815 F.3d 747 (Fed. Cir. 2016) ..	14
<i>Robert Bosch, LLC v. Snap-On Inc.</i> , 769 F.3d 1094 (Fed. Cir. 2014).....	26, 27
<i>Rowe Int'l Corp. v. Ecast, Inc.</i> , 586 F. Supp. 2d 924 (N.D. Ill. 2008).....	23, 25, 28

<i>Secure Web Conference Corp. v. Microsoft Corp.</i> , 2016 WL 626492 (Fed. Cir. 2016)	3
<i>Shatterproof Glass Corp. v. Libbey-Owens Ford Co.</i> , 758 F.2d 613 (Fed. Cir. 1985)	5
<i>Star Scientific, Inc. v. R.J. Reynolds Tobacco Co.</i> , 655 F.3d 1364 (Fed. Cir. 2011).....	5
<i>Teleflex, Inc. v. Ficosa N. Am. Corp.</i> , 299 F.3d 1313, 1328 (Fed. Cir. 2002).....	3
<i>Trading Techs. Int'l, Inc. v. eSpeed, Inc.</i> , No. 04 C 5312, 2006 WL 3147697 (N.D. Ill. Oct. 31, 2006), <i>clarified on denial of reconsideration</i> , No. 04 C 5312, 2007 WL 611258 (N.D. Ill. Feb. 21, 2007), and <i>aff'd</i> , 595 F.3d 1340 (Fed. Cir. 2010), and <i>aff'd</i> , 595 F.3d 1340 (Fed. Cir. 2010)	24, 26
<i>United States v. Telectronics, Inc.</i> , 857 F.2d 778 (Fed.Cir.1988)	23
<i>Verint Sys. Inc. v. Red Box Recorders Ltd.</i> , 166 F. Supp. 3d 364 (S.D.N.Y. 2016)	26, 27
<i>Versata Software, Inc. v. Sun Microsystems, Inc.</i> , No. 2:06-cv-358, 2008 WL 3914098 (E.D. Tex. Aug. 19, 2008)	24
<i>Vitronics Corp. v. Conceptronic, Inc.</i> , 90 F.3d 1576 (Fed.Cir.1996)	3, 4, 14
<i>Watts v. XL Sys., Inc.</i> , 232 F.3d 877 (Fed. Cir. 2000).....	22
<i>Williamson v. Citrix Online, LLC</i> , 792 F.3d 1339 (Fed. Cir. 2015) (<i>en banc</i>)	passim
<i>Zeroclick, LLC v. Apple Inc.</i> , No. 15-CV-04417-JST, 2016 WL 5477115 (N.D. Cal. Aug. 16, 2016)	26, 27

Statutes

35 U.S.C. §112(f).....	passim
------------------------	--------

TABLE OF EXHIBITS

Exhibit No.	Description	Appendix No.
A	Declaration of George Pazuniak in Support of Plaintiff SecurityProfiling LLC's Combined Opening and Responsive Claim Construction Brief	3-4
A-1	Data and Computer Security – Dictionary of standards concepts and terms	5-9
A-2	Prosecution history of '699 Patent - excerpt	10-11
A-3	US Patent No. 5,892,903	12-31
A-4	US Patent No. 6,298,445	32-50
A-5	US Patent No. 6,321,334	51-183
A-6	US Patent Application Publication No. 2002/0104014	184-215
A-7	US Patent Application Publication No. 2002/0026591	216-239
A-8	US Patent Application Publication No. 2002/0199122	240-252
A-9	US Patent Application Publication No. 2003/0014669	253-288

I. INTRODUCTION

The Parties currently dispute the constructions of 45 claim terms. By agreement of the Parties and with the Court's leave, this Brief combines Plaintiff's Opening and Responsive Claim Construction briefing. *See* D.I. 93.

The Supreme Court and the Federal Circuit have repeatedly held that it is the words of the patent's claims and disclosure that matter, and not the opinion of hired guns. Partially for this reason, Plaintiff submits that witness testimony at the *Markman* hearing is unnecessary and would be a counterproductive distraction from the intrinsic evidence, which cannot be contradicted by expert testimony.

Defendants have presented their proposed construction and supporting arguments of nine claim terms. D.I. 91 at 4-16. Additionally, Defendants propose that 36 additional claim terms, none of which contain the word "means," nevertheless be construed as means-plus-function claims under 35 U.S.C. §112(f). D.I. 91 at 18-30. Defendants propose, against the weight of considerable authority, that the words "code for" and "code that" are structureless "nonce" words synonymous with "means for." Defendants fail to rebut the presumption against means-plus-function construction which inheres when the word "means" is absent from the claims. Plaintiff respectfully requests the Court adopt its proposed constructions and reject those of Defendants.

II. THE PATENTS-IN-SUIT

At issue are six related patents, including U.S. Patent Nos. 8,266,699 ("the '699 Patent"); 8,984,644 ("the '644 Patent"); 9,100,431 ("the '431 Patent"); 9,117,069 ("the '069 Patent"); 9,118,708 ("the '708 Patent"); and 9,225,686 ("the '686 Patent") (collectively, "the Patents-in-Suit").

The Patents-in-Suit are directed to novel systems and methods for improving computer security as computing systems themselves become more complex. (See ‘699 patent, 1:30-46). Rather than, for example, simply relying on a large list of known attack signatures, the systems disclosed by the Patents-in-Suit typically begin by identifying vulnerabilities in a computer network, including vulnerabilities in specific devices and detecting attacks that could potentially take advantage of those vulnerabilities. Normally, these systems will use information gathered about software, policy settings, configurations, and patches for devices on the network (see, e.g., ‘699 Patent, 2:31-34) when making the determination as to whether a particular system is vulnerable or not (see, e.g., ‘699 patent, 4:5-26), along with a list of known security vulnerabilities and remediation or mitigation techniques (see, e.g., ‘699 patent, 2:35-46) The systems and methods also prevent or remediate the attacks, via user selectable techniques of various types, including patching, changing policy settings, and/or modifying configuration options. (See ‘699 Patent, 5:39-54).

Further, in specific embodiments, “a software development kit (SDK) allows programmers to develop security applications that access the data collected,” which may also include vulnerability and remediation information, using an application programming interface (API) to improve security-related decisions. (See ‘699 Patent, 5:30-43).

III. LEGAL STANDARD

A. General Rule of Claim Construction

Claim construction presents a question of law to be decided by the court. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 977-78 (Fed. Cir. 1995), aff’d, 517 U.S. 370, 388-90

(1996). “[T]he claims of a patent define the invention to which the patentee is entitled the right to exclude.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*) .

“Generally, claim terms should be given their ordinary and customary meaning from the perspective of a person having ordinary skill in the art at the time of the effective date of the patent application.” *Cioffi v. Google, Inc.*, 2015 WL 7254039 at *4 (Fed. Cir. 2015) .¹

In construing claims, courts rely primarily on the patent’s intrinsic evidence, which comprises the claims themselves, the patent specification and the patent’s prosecution history (if in evidence). *Phillips*, 415 F.3d at 1312–14.

It is a “cardinal sin” of patent law, however, to read limitations from the specification into the claims. *Philips*, 415 F.3d at 1319-20. The Federal Circuit “has repeatedly cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification.” *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1346-47 (Fed. Cir. 2015) (*en banc*) . “The patentee is entitled to the full scope of his claims, and [courts should] not limit him to his preferred embodiment or import a limitation from the specification into the claims.” *Kara Tech. Inc. v. Stamps.com Inc.*, 582 F.3d 1341, 1347-48 (Fed. Cir. 2009); *see also Avid Tech., Inc. v. Harmonic, Inc.*, 2016 WL 363410 at *5 (Fed. Cir. 2016); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1328 (Fed. Cir. 2002).

Indeed, “it is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited.” *Openwave Sys., Inc. v. Apple*

¹ *See also Secure Web Conference Corp. v. Microsoft Corp.*, 2016 WL 626492 at *2 (Fed. Cir. 2016) (citing *Phillips*, 415 F.3d at 1312–14, and *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed.Cir.1996)).

Inc., 808 F.3d 509, 514 (Fed. Cir. 2015) (quoting *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014)).

At times, a court may also rely on “extrinsic evidence,” which “consists of all evidence external to the patent and prosecution history,” including expert testimony. *Markman*, 52 F.3d at 980. However, “[i]n those cases where the public record unambiguously describes the scope of the patented invention, reliance on any extrinsic evidence is improper.” *Vitronics* at 1583 (emphasis added); *see also, Phillips*, 415 F.3d at 1318 (“conclusory, unsupported assertions by experts as to the definition of a claim term are not helpful to a court.”).

B. Law of Indefiniteness

Trend Micro asserts that many claim terms are “indefinite,” and, thus, is asking the Court to summarily invalidate those claims.

“Indefiniteness is a question of law . . . , subject to a determination of underlying facts.” *Akzo Nobel Coatings, Inc. v. Dow Chem. Co.*, 2016 WL 363443 at *8 (Fed. Cir. 2016). Patents are presumed to be valid, and the challenger bears the burden of establishing invalidity. *Id.* at *8.

Definiteness is evaluated based on a patent's specification and prosecution history, from the perspective of someone skilled in the relevant art at the time the patent was filed. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2128 (2014). The determination is whether “a patent's claims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty.” The definiteness requirement “recognize[es] that absolute precision is unattainable,” and “the certainty which the law requires in patents is not greater than is reasonable, having regard to their subject-matter.” *Nautilus*, 134 S. Ct. at 2129.

Thus, a “claim term may be definite even when discerning the meaning is a ‘formidable [task] and the conclusion may be one over which reasonable persons will disagree.’” *Star Scientific, Inc. v. R.J. Reynolds Tobacco Co.*, 655 F.3d 1364, 1373 (Fed. Cir. 2011) “If the claims, read in light of the specification, reasonably apprise those skilled in the art both of the utilization and scope of the invention, and if the language is as precise as the subject matter permits, the courts can demand no more.” *Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 624 (Fed. Cir. 1985).

A term that is well-understood in the art is not rendered indefinite, even if there are “a few inconsistent references in the specification,” because “if the terms at issue have ‘so clear an ordinary meaning, a skilled artisan would not be looking for clarification in the specification.’” *Cioffi* at *10 (quoting *Ancora Techs., Inc. v. Apple, Inc.*, 744 F.3d 732, 738 (Fed. Cir. 2014)).

Terms of degree are not indefinite provided the patent provides sufficient clarity to a skilled artisan. *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 126061 (Fed. Cir. 2014) (“the term ‘visually perceptible elements,’ or ‘look and feel elements that can be seen,’ viewed in light of the specification and prosecution history, informed those skilled in the art about the scope of the … patent’s claims with reasonable certainty.”); *Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1334–35 (Fed. Cir. 2010) (finding the phrase “not interfering substantially” to be definite where intrinsic evidence provided multiple examples that would allow a skilled artisan to determine scope of claim).

If there are genuine factual disputes as to what a person skilled in the art would have understood, the determination becomes a factual inquiry that, like obviousness, must now be resolved by a jury. *Cf., InTouch Technologies, Inc. v. VGO Commc’ns, Inc.*, 751 F.3d 1327, 1339 (Fed. Cir. 2014) (“Because obviousness is a mixed question of law and fact, ‘[w]e first

presume that the jury resolved the underlying factual disputes in favor of the verdict [] and leave those presumed findings undisturbed if they are supported by substantial evidence. Then we examine the [ultimate] legal conclusion [of obviousness] de novo to see whether it is correct in light of the presumed jury fact findings.””) (quoting *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1356–57 (Fed. Cir. 2012), which was quoting *Jurgens v. McKasy*, 927 F.2d 1552, 1557 (Fed. Cir. 1991)).

C. Means-Plus-Function Claiming

“Means-plus-function claiming occurs when a claim term is drafted in a manner that invokes 35 U.S.C. §112(f),² which states:”

An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

Williamson, 792 F.3d at 1347 (quoting 35 U.S.C. § 112(f)). The failure to use the word “means” creates a rebuttable presumption that §112(f) does not apply. *Id.* The Federal Circuit in *Williamson*, while expressly overruling previous holdings characterizing this presumption as “strong,” nevertheless reiterated that the absence of the word “means” places the burden of proof on the challenger seeking to invoke the effect of §112(f). *Id.* at 1348. “In making the assessment of whether the limitation in question is a means-plus-function term . . . the essential inquiry is . . . whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Id.* at 1349.

² Before the America Invents Act, 35 U.S.C. § 112(f) was contained in § 112 ¶ 6. *Driessen v. Sony Music Entm't*, 2016 WL 520263 at *2 (Fed. Cir. 2016). Thus, the cases cited in this brief often reference “§ 112 ¶ 6.” However, the law did not change, and § 112(f) and “§ 112 ¶ 6” can be used interchangeably.

“In construing means-plus-function claim limitations, a court must first define the particular function claimed. Thereafter, the court must identify the corresponding structure, material, or acts described in the specification.” *Budde v. Harley-Davidson, Inc.*, 250 F.3d 1369, 1376 (Fed. Cir. 2001) . “Failure to disclose adequate structure corresponding to the recited function in accordance with 35 U.S.C. § 112, ¶1, results in the claim being of indefinite scope, and thus invalid, under 35 U.S.C. § 112, ¶2.” *Id.* (citing *In re Dossel*, 115 F.3d 942, 945 (Fed. Cir. 1997)). “[A] challenge to a claim containing a means-plus-function limitation as lacking structural support requires a finding, by clear and convincing evidence, that the specification lacks disclosure of structure sufficient to be understood by one skilled in the art as being adequate to perform the recited function.” *Id.* at 1376-77 (“Because the claims of a patent are afforded a statutory presumption of validity, overcoming the presumption of validity requires that any facts supporting a holding of invalidity must be proved by clear and convincing evidence.”).

IV. DISPUTED TERMS TO BE CONSTRUED

For the Court’s convenience, Plaintiff divides the claims into those the Parties agree do not involving means-plus-function elements, and those that Defendants allege do. The numbering of the terms follows the numbering of terms in the Joint Claim Chart. D.I. 088-Ex A.

A. “Vulnerability”

Claim Term 1: “vulnerability”, “vulnerabilities”, “device vulnerability”, “device vulnerabilities” and similar terms (all Patents-in-Suit)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“Vulnerability”: A security weakness, gap or flaw that could be exploited by an attack or threat.	A device configuration (including installed software) that can be exploited by an attack against [a/the] device

“Device Vulnerability” and Similar Terms: No further construction is required after “vulnerability” is construed.	
---	--

Both parties agree that vulnerabilities require something can or could “be exploited by an attack.” The intrinsic and extrinsic evidence support SecurityProfiling’s position that this term should be construed to be “a security weakness, gap or flaw that could be exploited by an attack or threat,” making it clear that devices may have vulnerabilities based on various factors, including their current configurations. Conversely, Trend Micro’s construction mischaracterizes evidence in an attempt to equate a **vulnerability** with a device that may **have** a vulnerability.

SecurityProfiling’s construction accords with the customary meaning of “vulnerability,” and is consistent with the claim language and the specification. Trend Micro’s construction is erroneous for two reasons: Trend Micro limits a vulnerability to a “device configuration,” and further limits the construction to vulnerabilities that attack “devices.”

The claim language itself supports SecurityProfiling’s position. Claim 1 of the ‘644 patent, for example, states “determining that [a] plurality of devices is actually vulnerable to at least one actual vulnerability based on [an] identified at least one configuration.” Thus, the relevance of “devices” and “configurations” is already elsewhere specifically provided for in the claim, which means that the patent separated out the terms “vulnerability” from the terms “device” “configuration.” There is no reason to burden the common term “vulnerability” by importing other elements.

Second, Trend Micro’s construction renders that “644 Patent claim 1 internally inconsistent. Trend Micro construes “vulnerabilities” as being the device configurations. But

claim 1 states that the “actual vulnerability [is] **based on** the identified at least one configuration.” The concept of “vulnerability is the device configuration” is very different from the concept of a vulnerability being “based on” a device configuration. The claims do not limit a vulnerability to merely a device configuration.

The specification also supports SecurityProfiling’s position. For example, the ‘699 Patent states “the system presents a user with the list of remediation techniques available **to protect against a known vulnerability**” (‘699 Patent, Abstract (emphasis added)). Protecting against a known device configuration, as Trend Micro would propose, makes no sense. However, protecting against a known security weakness, as SecurityProfiling proposes, does. Further, the Specification discloses that system can apply a remediation technique “to all devices subject to the same vulnerability (based on their real-time software, patch, policy, and configuration status)” ‘699 Patent, 4:61-65. This clearly illustrates Trend Micro’s proposed construction is incorrect - it explicitly states that a vulnerability is different than a configuration. The vulnerability is **based** on various factors, including configuration, and therefore a vulnerability cannot BE a configuration.

The extrinsic evidence further supports SecurityProfiling’s position. The reference book, “Data & Computer Security: Dictionary of standards concepts and terms,” defines vulnerability as follows:

vulnerability. (1) In computer security, **a weakness in automated system security procedures, administrative controls, internal controls, etc. that could be exploited** by a threat to gain unauthorized access to information or to disrupt critical processing. (AFR). (2) In computer security, **a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited** to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. ... (3) **In computer security, any**

weakness or flaw existing in a system. The susceptibility of a system to a specific threat attack or harmful event, or the opportunity available to a threat agent to mount that attack.

Ex. A-1, *Data & Computer Security: Dictionary of standards concepts and terms*, p. 366 (emphasis added). Trend Micro mischaracterizes the evidence it provides and points to. For example, Trend Micro notes that “The Trend Micro glossary cited by SecurityProfiling similarly confirms that vulnerabilities are tied to a device’s configuration and installed software. *See* Ex. 1-C at A135 (vulnerabilities are ‘found in programs and operating systems leaving computing systems open to malware and hacker attack’).” *See* D.I. 91, p. 7. However, the quoted portion skips several introductory words in order to paint a completely different picture than what was intended. Vulnerabilities are not “tied to a device’s configuration and installed software,” or limited merely to aspects “found in programs and operating systems” The entire sentence they quote reads “A vulnerability is a security weakness typically found in programs and operating systems leaving computer systems open to malware and hacker attack.” Using a traditional understanding of English grammar, or simply ignoring the exemplary language, this sentence shows just how broadly vulnerability is used - a vulnerability is “a security weakness ... [that] leav[es] computer systems open to malware and hacker attack.” Programs and operating systems are just examples of locations where vulnerabilities may exist. It is clear that from as far back as 1989 through the time at which the referenced Trend Micro glossary was written, a person skilled in the art would understand vulnerabilities were not limited to merely device configurations that could be exploited in attacks against the device, but rather encompassed *any* weakness, including weaknesses in procedures, external and internal controls, physical layout, personnel, hardware or software in the entire system that could be exploited.

B. “Intrusion Prevention System”

Claim Term 2: "Intrusion Prevention System" ('644, '686, '069, '431, and '708 Patents)	
Plaintiffs' Proposed Construction	Defendants' Proposed Construction
"A system that monitors and processes network traffic to detect and prevent vulnerability exploits"	"A system that monitors and processes packets in network traffic to detect and prevent vulnerability exploits by dropping malicious packets in real time"

Both parties agree that an intrusion prevention system is "a system that monitors and processes ... network traffic to detect and prevent vulnerability exploits" However, Trend Micro's construction improperly imports limitations from examples in the Specification into its construction of the claim limitation.

First, it is generally erroneous to provide claim constructions that are inconsistent with the specification. Trend Micro does exactly that here. Thus, the specification and claims repeatedly refer to the use of firewalls as part of the intrusion prevention system. A firewall, even as defined by Trend Micro, is a "barrier." A firewall, by Trend Micro's own definition, will block traffic that "does not conform to pre-configured rules."³ There is no requirement that a firewall "monitor and process packets." Thus, Trend Micro's proposed construction may effectively preclude firewalls from being considered to be components of an intrusion prevention system, even though the specifications and claims include firewalls as such.

Second, the intrinsic evidence does not support the narrow construction offered by Trend Micro. The claims themselves make it clear that the scope of an intrusion prevention system is not limited to merely "monitor[ing] and process[ing] packets" and then "dropping malicious packets in real time" as proposed by Trend Micro. Specifically, claim 1 of the '644 patent recites "**identifying** an occurrence in connection with at least one of the plurality of devices ... [and

³ <https://www.trendmicro.com/vinfo/us/security/definition/firewall> from certain sites, without monitoring and processing "packets."

selectively using] an *intrusion prevention system*-based occurrence mitigation type ... for occurrence mitigation *by preventing advantage being taken of actual vulnerabilities*” The ‘686 Patent, claim 10, recites a similar limitation:

code that utilizes the intrusion prevention system component to, after receipt of the intrusion prevention system rule and after identification of the occurrence capable of taking advantage of the actual vulnerability addressed by the intrusion prevention system rule, prevent the actual vulnerability addressed by the intrusion prevention system rule from being taken advantage of.

Thus, the claim language itself merely requires the system be capable of detecting and preventing vulnerability exploits. Nothing in the various specifications would narrow this scope - the inventors did not act as their own lexicographer, and nothing in the specifications disclaimed or disparaged this broad scope. Certainly, the specification indicates the term “intrusion prevention system” encompasses real time responses (*see, e.g.*, ‘644 patent, 19:8-10 (“In one embodiment an intelligent IPS may be provided that provides intelligence, accuracy, real-time prevention, and remote patching functions.”)). However, these are simply examples of potential embodiments, rather than requirements.

C. “Firewall”

Claim Term 3: “Firewall” (‘644, ‘686, ‘069, ‘431, and ‘708 Patents)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“A security system to protect against external threats, that acts as a barrier through which information passing between external systems and one or more networks must travel”	“A security system to protect against external threats, that acts as a barrier through which all information passing between external systems and one or more networks must travel”

The parties generally agree on the definition of “firewall,” save that Trend Micro wishes to add a completely unsupported limitation that “*all* information” passing between external systems and one or more networks must pass through the firewall.

Whether any or all information passes through a firewall is a network design decision; in some instances, a network may have all network assets protected behind a firewall, while in

other instances, a network may need, or may otherwise find benefit, in allowing certain assets to remain unprotected by a firewall. A firewall cannot be defined by limiting what network configurations the firewall can be used within.

Nothing in the claims or specification limits the firewall to a specific network configuration. Even Trend Micro's proposed extrinsic evidence supports this position: “*Firewall: A firewall prevents computers on a network from communicating directly with external computer systems.* A firewall *typically* consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules.” (Microsoft Computer Dictionary, 3d ed., 1997) (emphasis added). Even the Microsoft Computer Dictionary definition relied on by Trend Micro indicates the sole purpose of a firewall is to prevent direct communication between a device on one side of the firewall with a device on the other. Simply because a firewall is typically configured in a particular fashion does not require that it always be configured in such a way.⁴

Trend Micro is clearly trying to import elements from some of the simplified embodiments used to describe the invention into the claim limitations.

D. “Remediation Technique”

Claim Term 4: “Remediation Technique” (‘699 Patent)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
An action that corrects or counteracts a vulnerability, including the closing of open	“An action that makes changes to a device to correct a vulnerability on the device”

⁴ Trend Micro quotes from the Trend Micro glossary cited to by SecurityProfiling but, as it has done consistently in its opening brief, states exemplary language as definitive language. Here, Trend Micro ignore the word “typically” in the portion it quotes to describe how a firewall is typically configured. *See* D.I. 91, pp. 10-11.

ports on the device; installation of a patch that is known to correct the vulnerability; changing the device’s configuration; stopping, disabling, or removing services; setting or modifying policies; registry settings or changes; updates to machines; or the like”	
---	--

Trend Micro wishes to improperly limit the scope of the claim term to only those that actions that cause a change on the device itself, and only to *correct* vulnerabilities. The intrinsic evidence fully supports Security Profiling’s proposed construction.

First, when describing Figure 3, the ‘699 patent states that in one embodiment, after a security server determines if a computer is vulnerable to a particular attack, the security server signals back to the firewall whether a connection request should be granted, and if not, the firewall “drops or rejects the connection request … as is understood in the art.” See ‘699 patent, 4:27-35. Thus, at least for this embodiment, the vulnerability is remediated with a firewall policy or configuration that drops or rejects the connection request. Said differently, the remediation technique encompasses not just making changes to a vulnerable device to make it invulnerable, but also encompasses having the system counteract the vulnerability. Further, it should be noted that the embodiment described in Fig. 3 is a preferred embodiment. See ‘699 patent, 5:26-29. And, as The Federal Circuit has “often remarked that a construction which excludes the preferred embodiment is ‘rarely, if ever correct.’” *PPC Broadband, Inc. v. Corning Optical Commc’ns RF, LLC*, 815 F.3d 747, 755 (Fed. Cir. 2016) (quoting *Vitronics*, 90

F.3d at 1583). Here, Trend Micro’s proposed construction would exclude the preferred embodiment, and thus, there is at least a presumption that such a construction would be incorrect.

Second, the ‘699 patent clearly defines a scope that includes more than simply “making changes to a device”. The ‘699 patent states: “[i]n various embodiments, remediation techniques *include the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device’s configuration; stopping, disabling, or removing services; setting or modifying policies; and the like.*” ‘699 Patent, 5:1-5. In other words, SecurityProfiling’s proposed construction utilizes the exact words the inventors used to define the scope of the term.

E. “Each mitigation technique has a mitigation type including at least one of a patch, a policy setting, [and/or] a configuration option”

Claim Term 5: “Each mitigation technique has a mitigation type including at least one of a patch, a policy setting, [and/or] a configuration option” (‘708 and ‘431 Patents)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“The mitigation techniques must include at least one of a patch, policy setting, or configuration option type, but otherwise not limited to those types”	“The mitigation techniques must include each of a patch, policy setting, and configuration option type”

The two parties disagree with respect to whether the language of the claim term requires the use of just one mitigation type, or if it must include all three types.

Even before looking at intrinsic and extrinsic evidence, the grammar used and the plain and ordinary meaning of the words, on their face, clearly indicates to one of skill in the art that SecurityProfiling’s proposed construction is correct. The claim term first requires that each mitigation technique must have a mitigation type. One of skill in the art would recognize that the mitigation types are somewhat unique, and a given mitigation technique would not be all three – for example, dropping or rejecting a packet is clearly either a policy setting or configuration option, but is not a patch. Similarly, installing a software patch for vulnerable software is clearly just a patch and not a policy setting. Thus, each mitigation technique cannot be all three types,

simultaneously. The claim term itself goes on to require that each mitigation type must be at least one of the three listed types – patch, policy setting, and configuration option. Therefore, it is readily evident from the grammar, and from the plain and ordinary meaning of the terms, that at least in some cases, each mitigation technique may be the same, single mitigation type (e.g., a “patch”), and thus the system does not require that the mitigation techniques include all three types.

The intrinsic evidence also supports this position. For example, dependent claim 17 of the ‘708 patent recites a system “wherein the computer program product is operable such that at least one of: said mitigation type include the patch … said mitigation type includes the policy setting; [and] said mitigation type includes the configuration option.” By including a dependent claim that called out inclusion of each mitigation type, separately, it is clear the independent claim (here, claim 4) is intended to also cover scenarios in which one or more of those limitations was not present. Further, starting in the Abstract, the Specification states that “each remediation technique has a remediation type selected from the type group consisting of patch, policy setting, and configuration option.” *See* ‘708 Patent, Abstract; 1:31-35. Thus, one of skill in the art examining the intrinsic evidence, would understand that the mitigation techniques must include at least one of the identified types of mitigation techniques, but would not require all of the mitigation techniques to be present.

Trend Micro also attempts to make an enablement argument under the guise of indefiniteness. Trend Micro argues that claims in the ‘708 and ‘431 Patents are indefinite, asserting that a mitigation technique cannot be classified as a particular type of technique (patch, policy setting, or configuration option) and also be performed by a particular structure (i.e., firewall and/or intrusion prevention system). This is clearly incorrect - one of skill in the art

would readily understand, for example, that a firewall, for example, could use a mitigation technique such as dropping or rejecting a connection request, and that such a technique would be classified as a policy setting (i.e., the policy of the firewall and/or IPS) or configuration option (i.e., how the firewall and/or IPS are configured to respond). *See, e.g.*, ‘708 patent, 4:13-21.

F. “Each remediation technique has a remediation type selected from the group consisting of a patch, a policy setting, and a configuration option”

Claim Term 6: “Each remediation technique has a remediation type selected from the group consisting of a patch, a policy setting, and a configuration option” (‘699 Patent)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“The remediation techniques must include at least one of a patch, policy setting, or configuration option type, but otherwise not limited to those types”	“The remediation techniques must include at least one of a patch, policy setting, or configuration option type, without any other types”

Similar to Claim Term 5, above, the two parties disagree with respect to whether the language of the claim term requires the use of just one remediation type, or if it must include all three types, and whether the remediation techniques may include other types beyond those indicated by the “group consisting of a patch, a policy setting, and a configuration option.”

Even before looking at intrinsic and extrinsic evidence, the grammar used and the plain and ordinary meaning of the words, on their face, clearly indicates to one of skill in the art that SecurityProfiling’s proposed construction is correct. The claim term first requires that each remediation technique must have a remediation type. One of skill in the art would recognize that the remediation types are somewhat unique, and a given remediation technique would not be all three – for example, dropping or rejecting a packet is clearly either a policy setting or configuration option, but is not a patch. Similarly, installing a software patch for vulnerable software is clearly just a patch and not a policy setting. Thus, each remediation technique

cannot be all three types, simultaneously. The claim term itself goes on to require that each remediation type must be at least one of the three listed types – patch, policy setting, and configuration option. Therefore, it is readily evident from the grammar, and from the plain and ordinary meaning of the terms, that at least in some cases, each remediation technique may be the same, single remediation type (e.g., a “patch”), and thus the system does not require that the remediation techniques include all three types.

The intrinsic evidence also supports this position. For example, dependent claim 2 of the ‘708 patent recites a system “wherein the computer program product is operable such that at least one of: said remediation type include the patch ... said remediation type includes the policy setting; [and] said remediation type includes the configuration option.” By including a dependent claim that called out inclusion of each remediation type, separately, it is clear the independent claim (here, claim 4) is intended to also cover scenarios in which one or more of those limitations was not present. Further, starting in the Abstract, the Specification states that “each remediation technique has a remediation type selected from the type group consisting of patch, policy setting, and configuration option.” *See* ‘708 Patent, Abstract; 1:31-35. Thus, one of skill in the art examining the intrinsic evidence, would understand that the remediation techniques must include at least one of the identified types of remediation techniques, but would not require all of the remediation techniques to be present.

G. “Occurrence”

Claim Term 7: “Occurrence” (‘644, ‘069, and ‘686 Patents)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“Any attempt to expose, deny, degrade, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of a computer network”	“Malicious packets targeting a device detected in network traffic”

SecurityProfiling’s proposed construction is supported by the intrinsic evidence, while Trend Micro’s proposed construction can only be reached via a mischaracterization of the Specification.

The patent specifications use “occurrence” synonymously with “attack.” (1:25-37). An “attack” is generally-recognized by those skilled in the art to mean “any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.”⁵

Trend Micro continues to attempt to erroneously limit the claims to “malicious packets” rather than to any attack. First, Trend Micro attempts to limit occurrence to those actually detected in network traffic. The claim language itself requires “identifying an occurrence” which implies that there are unidentified, and therefore undetected, occurrences. For example, the Specification of the ‘644 patent states that “[a]dditionally, blended attacks may now utilize metamorphic or polymorphic abilities to change their signatures to avoid detection.” (‘644 patent, 8:11-13). Thus, one of skill in the art will recognize that an occurrence may take place without anyone knowing about it until later when, for example, previously secure information is found to have been leaked, altered, or otherwise made unsecure. Thus, an occurrence may take place that is not detected in network traffic. Rather, it is clear that an occurrence is an attempt to gain access to the system - to expose, deny, degrade, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of a computer network – via a vulnerability in at least one device.

⁵ Support:
[https://en.wikipedia.org/wiki/Attack_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing)) ;
<https://www.techopedia.com/definition/6060/attack>;
<https://www.thefreedictionary.com/computer+network+attack>

Second, the patent states that the invention is designed to protect systems from, for example, “viruses, worms, and denial of service attacks” and “new blended attacks.” (‘644 Patent at 8:9-11). These attacks comprise “malicious packets,” but are not necessarily limited to them.

Third, any computer network is comprised of devices. Without devices, there is no computer network. The claimed occurrences are directed to one or more devices. (See ‘644 Patent, claim 1 (“identifying an occurrence in connection with at least one of the plurality of devices”); ‘431 Patent, claim 1 (“identifying an attack in connection with the at least one device”); ‘069 Patent, claim 2 (“identifying: in connection with the at least one networked device, a first occurrence including at least one first occurrence packet directed to the at least one networked device”)). But one of skill in the art would understand that gaining access to a particular device may also allow access to other devices on that network, and thus an occurrence must necessarily include more than simply access to a particular device, but rather access to the computer network as a whole.

Fourth, the claims themselves differentiate between the occurrence and the occurrence packet. Claim 1 of the ‘069 patent, for example, recites “reporting at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability ...” While the occurrence packet may be directed to a networked device, the occurrence may in fact be more than just an occurrence packet. Thus, the occurrence cannot be restricted merely to one of the parts – the at least one first occurrence packet - that comprises the occurrence.

The patent specifications disclose that the intrusion prevention system seeks to limit “malicious packets,” but nothing in the patent specifications limits “occurrences” to malicious packets.”

H. “Occurrence Packet”

Claim Term 8: “Occurrence Packet” (‘069 Patent)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
“A packet that is part of an occurrence”	“A packet that is part of an occurrence detected in network traffic” ^[1] _[SEP]

The parties agree that an occurrence packet is a packet that is part of an occurrence. However, Trend Micro adds an additional limitation; that the packet must also be detected in network traffic. The intrinsic evidence supports SecurityProfiling’s position.

Specifically, claim 1 recites “determining: that *the first occurrence including the at least one first occurrence packet*” Thus, the claim term is simply a packet that is part of an occurrence. There is no support for requiring additional restrictions (i.e., that it must be detected in network traffic), or, alternatively, additional restrictions that are, or could be, included are merely those a skilled artisan would understand as inherent in systems that communicate via packets.

I. “Attack”

Claim Term 8: “Occurrence Packet” (‘069 Patent)	
Plaintiffs’ Proposed Construction	Defendants’ Proposed Construction
No construction needed, but, in the alternative, “attack” should have same construction as “occurrence”	“Malicious packets targeting a device detected in network traffic”

The term “attack” is readily recognizable to a skilled artisan and should not need construction. *See n.5., supra.* However, if a construction is required, the construction of

“occurrence” is a suitable alternative because the patents refer to “occurrences” and “attacks” interchangeably, and in each case meaning “attack.”

V. CLAIM TERMS DEFENDANT ALLEGES ARE GOVERNED BY 35 U.S.C. § 112(f)

Defendants assert that some 36 claim terms (Claim Terms 10 – 45), none of which include the word “means,” should be governed nevertheless by §112(f). The parties have agreed on seven groupings of the allegedly mean-plus-function terms based on common subject matter as presented in the Joint Claim Construction Statement. The groupings reflect common issues for related terms and are drawn to reduce the number of questions for the Court.

A. Absence of the noun “means” from the disputed claims creates a presumption that §112(f) does not apply.

At the threshold, none of the disputed claim terms contains the word “means,” creating a presumption that they are not governed by the functional claiming provision of 35 U.S.C. § 112(f). *See Personalized Media Communications, LLC v. International Trade Commission*, 161 F.3d 696, 703–04 (Fed. Cir. 1998) . To determine whether § 112(f) applies to a claim limitation, Federal Circuit precedent “has long recognized the importance of the presence or absence of the word ‘means.’” *Williamson*, 792 F.3d at 1348. In *Williamson*, the Federal Circuit overruled previous holdings characterizing this presumption as “strong,” but nevertheless maintained the burden of proof on a challenger seeking to invoke the effect of §112(f). *Id.* “When a claim term lacks the word ‘means,’ the presumption can be overcome and § 112, para. 6 will apply if the challenger demonstrates that the claim term fails to ‘recite sufficiently definite structure’ or else recites ‘function without reciting sufficient structure for performing that function.’” *Id.* (citing *Watts v. XL Sys., Inc.*, 232 F.3d 877, 880 (Fed. Cir. 2000)).

Defendants seek to overcome the presumption by misrepresenting and distorting the governing case law. Contrary to Trend Micro’s assertion, the Federal Circuit in *Williamson* construed the word “module,” not “code,” and did not mention or analogize the word “code.”

A claim term does not fall under § 112(f) if it “is used in common parlance or by persons of skill in the pertinent art to designate structure, *even if the term covers a broad class of structures and even if the term identifies the structures by their function.*” *Lighting World, Inc. v. Birchwood Lighting, Inc.*, 382 F.3d 1354, 1359-60 (Fed. Cir. 2004) (emphasis added). The Federal Circuit’s decision in *Williamson* has not changed this standard.⁶ See *Williamson* at 1349 (citing *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1584 (Fed.Cir.1996)) (“The standard is whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.”). Further, in their effort to analogize to the “module” in *Williamson*, Defendants focus on the word “code” in isolation, which is improper. The Court should not “read terms in isolation; it must consider the limitations as a whole.” *Rowe Int'l Corp. v. Ecast, Inc.*, 586 F. Supp. 2d 924, 944–45 (N.D. Ill. 2008) (citing *Apex Inc. v. Raritan Computer, Inc.*, 325 F.3d 1364, 1372, 1374 (Fed. Cir. 2003) (citing *United States v. Telecommunications, Inc.*, 857 F.2d 778, 781 (Fed.Cir.1988)) (finding error in district court’s “reliance on single words of the limitations … as opposed to the limitations as a whole” in its determination that the limitations at issue were means-plus-function limitations))). The Federal Circuit has never identified “code,” “code for,” or “code that” as a non-structural,

⁶ The *Williamson* court reduced but did not eliminate the evidentiary requirement for rebuttal of the presumption against the application of § 112, ¶ 6: “Henceforth, we will apply the presumption as we have done prior to *Lighting World*, without requiring any heightened evidentiary showing and expressly overrule the characterization of that presumption as ‘strong.’ We also overrule the strict requirement of ‘a showing that the limitation essentially is devoid of anything that can be construed as structure.’” *Williamson*, 792 F.3d at 1349.

“nonce” word, or affirmed the application of § 112(f) to a claim on the basis that “code” is synonymous with “means.”

In fact, Courts have regularly rejected Trend Micro’s argument, and have held that “code for” does not signal a means-plus-function element. See, for example, *Affymetrix, Inc. v. Hyseq, Inc.*, 132 F. Supp. 2d 1212, 1232 (N.D. Cal. 2001), where the Court stated:

The Court finds that “computer code” is not a generic term, but rather recites structure that is understood by those of skill in the art to be a type of device for accomplishing the stated functions. **** “[C]omputer code” is more similar to terms like “detent mechanism” and “digital detector,” than “element,” “means,” or “device.”

See also Versata Software, Inc. v. Sun Microsystems, Inc., 2008 WL 3914098 (E.D. Tex. 2008) (holding that § 112 ¶ 6 does not apply to the claim term “computer readable program code configured to cause a computer to [perform a function]”); *Aloft Media, LLC v. Adobe Sys.*, 570 F. Supp. 2d 887, 897– 98 (E.D. Tex. 2008) (holding that § 112, ¶ 6 does not apply to the claim term “computer code for [performing a function]”); *Eolas Techs., Inc. v. Adobe Sys., Inc.*, 810 F. Supp. 2d 795, 810 (E.D. Tex. 2011) (finding that where claim “element[s] asserted by Defendants includes a phrase containing either the words ‘computer readable program code for ...’ or ‘software comprising computer executable instructions [to] ...’ followed by a description of the code’s (or software’s) operation,” the “code and software in the claims describe[d] sufficient structure to avoid the application of § 112, ¶ 6.”), *opinion withdrawn in part on reconsideration*, No. 6:09-CV-446, 2011 WL 11070303 (E.D. Tex. Sept. 23, 2011), and *aff’d sub nom. Eolas Techs. Inc. v. Amazon.com, Inc.*, 521 F. App’x 928 (Fed. Cir. 2013); *RLIS, Inc. v. Allscripts Healthcare Solutions, Inc.*, 2013 WL 3772472 (S.D. Tex. 2013) (holding that § 112 ¶ 6 does not apply to the claim terms “executable software [for performing a function]” and

“computer software for [performing a function]”); *Affinity Labs of Texas, LLC v. Samsung Elecs. Co.*, 2014 U.S. Dist. LEXIS 184075, at *11–*18 (E.D. Tex. 2014) (holding that § 112 ¶ 6 does not apply to the claim term “software... configured to [perform a function]”); *SuperSpeed, LLC v. Google, Inc.*, 2014 WL 129225 (S.D. Tex. 2014) (holding that § 112, ¶ 6 does not apply to the claim term “executable...code for [performing a function]”); *Syncpoint Imaging, LLC v. Nintendo of Am. Inc.*, 2016 WL 55118 at *23 (E.D. Tex. 2016); *Chamberlain Grp., Inc. v. Lear Corp.*, 756 F. Supp. 2d 938, 976–77 (N.D. Ill. 2010) (finding “code-generator elements connote a structure to one skilled in the art”); *Convolve, Inc. v. Dell, Inc.*, No. 2:08-CV-244-CE, 2011 WL 31792, at *18 (E.D. Tex. Jan. 5, 2011) (“The ‘code to ...’ and ‘code providing ...’ limitations of [the] claims . . . recite structure and thus are easily distinguishable.”), *opinion clarified*, No. 2:08-CV-244-CE, 2011 WL 13089002 (E.D. Tex. July 5, 2011); *Rowe Int'l Corp.* 586 F. Supp. 2d at 944–45 (“[A] person of ordinary skill in the relevant field would recognize sufficient structure, in the form of instructions located within a memory, to perform the recited functions.”); *Trading Techs. Int'l, Inc. v. eSpeed, Inc.*, No. 04 C 5312, 2006 WL 3147697, at *10–13 (N.D. Ill. Oct. 31, 2006) (finding claim containing the term “program code” “recite[d] sufficiently definite structure to avoid the ambit of § 112, ¶ 6”), *clarified on denial of reconsideration*, No. 04 C 5312, 2007 WL 611258 (N.D. Ill. Feb. 21, 2007), and *aff'd*, 595 F.3d 1340 (Fed. Cir. 2010), and *aff'd*, 595 F.3d 1340 (Fed. Cir. 2010).

The court in *Trading Techs. Int'l, Inc.* stated:

The term “code,” with regard to computer technology, is defined as: “In software engineering, computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator.” The New IEEE Standard Dictionary of Electrical and Electronics Terms, Fifth Ed. (1993). Such a definition is not a “generic structural term such as ‘means,’ ‘element,’ or ‘device’; nor is it a coined term lacking a clear meaning, such as ‘widget’ or ‘ram-a-fram.’”

Trading Techs. Int'l, Inc. at *12 (quoting *Personalized Media Communications, LLC*, 161 F.3d at 704).

The cases cited by Trend Micro are entirely distinguishable and do not support Trend Micro's proposition. In addition to *Williamson*, Trend Micro relies principally on *Robert Bosch, LLC v. Snap-On Inc.*, 769 F.3d 1094, 1099–102 (Fed. Cir. 2014); *Zeroclick, LLC v. Apple Inc.*, No. 15-CV-04417-JST, 2016 WL 5477115, at *3–5 (N.D. Cal. Aug. 16, 2016); *Zeroclick, LLC v. Apple Inc.*, No. 15-CV-04417-JST, 2016 WL 5477115 (N.D. Cal. Aug. 16, 2016); *Verint Sys. Inc. v. Red Box Recorders Ltd.*, 166 F. Supp. 3d 364, 378–86 (S.D.N.Y. 2016).

The Federal Circuit in *Williamson* addressed, *inter alia*, the construction of the claim term “distributed learning control module.” The court described the word “module” as “a well-known nonce word that can operate as a substitute for ‘means,’” aided in this conclusion by the plaintiff who himself acknowledged that “the term ‘module,’ standing alone is capable of operating as a ‘nonce word’ substitute for ‘means.’” *Williamson*, 792 F.3d at 1350-51. Further, the court concluded that neither the prefix “distributed learning control” nor the written description “provide[d] any structural significance” to the term. *Id.* at 1351. As already argued in detail, the disputed terms in this case rest on a much more definite structural foundation than the “distributed learning control module” in *Williamson*. *See* V.B.1. - V.B.7., *infra*. In contrast to the instant case, the appellant in *Williamson* failed to present persuasive evidence that a “distributed learning control module” would be understood by an ordinarily skilled artisan as a name for structure. *Williamson* at 1351. Moreover, in contrast to “module,” the Federal Circuit has never held the word “code” to be “a well-known nonce word that can operate as a substitute for ‘means.’” Defendants’ reliance on *Williamson* is unavailing.

Defendants' reliance on *Bosch* is similarly misplaced. The Federal Circuit in *Bosch* construed claim terms "program recognition device" and "program loading device." *Bosch* at 1099. The court noted that it had already identified "device" as a "non-structural, 'nonce' word." *Id.* Moreover, the specification of the patent in question did not contain "a single reference to the structure of the 'program recognition device' itself," and was "silent about how the 'program loading device' receives and processes signals." *Id.* at 1099-1100. By contrast, the disputed terms in this case rest on a much more definite structural foundation than the "program devices" in *Bosch*. *See* V. B.1. - V.B.7., *infra*. Further, and as stated with respect to *Williamson*, the Federal Circuit has never identified "code," "code for," or "code that" as a non-structural, "nonce" word, or affirmed the application of § 112(f) to a claim on the basis that "code" is synonymous with "means."

The district court in *Zeroclick* applied § 112(f) to the terms "program that can operate the movement of the pointer (0)" and "user interface code," analogizing them to the "module" in *Williamson*. *Zeroclick* at *6-7. Similar to *Bosch*, and again in contrast to the instant case, neither additional claim language nor the patent specification in *Zeroclick* provided additional structure on which the disputed terms could rest. *Id.* Lastly, the court in *Verint* applied § 112(f) to the terms "first computer application operative" and "monitoring system operative," on much the same grounds: "'System' standing alone is a nonce word that does not describe a structure that could perform the listed functions and the modifier 'communication monitoring' provides a functional description of the system but no structure. Neither does the description of the 'monitoring system' in the specification point to a sufficiently definite structure to save [the] claim." *Verint* at 381. By contrast, in this case the word "code" is lent structural significance by

a substantial number of additional claim terms which are understood by an ordinarily skilled artisan as being names for structure. *See* V.B.1. - V.B.7., *infra*.

B. Defendants cannot rebut the presumption that § 112(f) does not apply merely by labeling “code” a nonce term synonymous with “means.”

Defendants cannot distinguish the limitations here from the “code” limitations that the Courts have regularly held to be not governed by § 112(f). The limitations argued by Trend Micro require a “computer program product embodied on a non-transitory computer readable medium” that includes the “code for” – instruction set – followed by a detailed description of what the code or instruction set does. As held in the aforesaid cases, such “code” limitations connote a structure to one skilled in the art. Trend Micro has not distinguished this established law. Thus, § 112(f) cannot apply.

Although it is apparent that Trend Micro’s arguments contradict well-established law and § 112(f) cannot apply, in the exercise of caution, SecurityProfiling will further analyze the limitations to demonstrate that, even if the word “code” could be considered a nonce word, the disputed claims recite additional structure for performing the claimed functions, which would readily be recognized by a person of skill in view of the patent specification.

1. Claim Terms Concerning Multiple Mitigation Techniques (Claim Terms 10-23)

None of claim terms 10 – 45 contains the word “means,” creating a presumption against the application of §112(f). *Williamson*, 792 F.3d at 1348. Further, when considered “as a whole” these claim terms contain words understood by an ordinarily skilled artisan “to have a sufficiently definite meaning as the name for structure.” *Id.* at 1349; *Rowe* at 944-45. These words explain and give structure to the words “code for” and “code that.” Words understood by

an ordinarily skilled artisan “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “intrusion prevention system,” “firewall,” “software update,” and “user input.”

a. *intrusion prevention system* (Claim Terms 10, 13, 14, 19, 20-23)

An ordinarily skilled artisan would comprehend *intrusion prevention system* as a term indicating structure. An *intrusion prevention system* is disclosed in the specification of the ‘644 Patent. 7:14, 10:29 (intrusion detection system “IDS”); Figs. 5b, 12 (IDS). Further, an *intrusion prevention system* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *intrusion prevention* or *detection* and closely related concepts. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-3 (US Patent No. 5,892,903, Fig. 2 (IP spoofing attack detection)); Appendix A-4 (US Patent No. 6,298,445, 4:24-32; Fig. 1 (network security detector 16); 6:52-56; Fig. 2 (Network security detector 16 including intruder detector 48)). Thus, *intrusion prevention system* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

b. *firewall* (Claim Terms 11, 13, 15, 19, 20-23)

An ordinarily skilled artisan would comprehend *firewall* as a term indicating structure. A *firewall* is disclosed repeatedly in the specification of the ‘644 Patent. 3:12-26; 4:13-21; Fig. 2 (Firewall 131); Fig. 3 (Firewall 131); Fig. 5b (Firewall); Fig. 12 (Firewall). Further, *firewall* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit

claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *firewalls*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-3 (US Patent No. 5,892,903, 3:22-29); Appendix A-4 (US Patent No. 6,298,445, 4:22-24; Fig. 1 (firewall 12)); Appendix A-5 (US Patent No. 6,321,334, 13:14-37; Fig. 2 (firewall 212)); Appendix A-9 (US Patent Application Publication No. 2003/0014669, [0056]). Thus, *firewall* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

c. *software update* (Claim Terms 12, 13, 16)

An ordinarily skilled artisan would comprehend *software update* as a term indicating structure. *Software updating* is disclosed in the specification of the ‘644 Patent. 2:1-3; Fig. 8. Further, *software update* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to a patent issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which makes reference to or disclose *software updates*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-4 (US Patent No. 6,298,445, 7:37-54 (providing software enhancements); Table 1 (Patch)). Thus, *software update* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

d. *user input* (including *selection by . . . user*) (Claim Terms 10-23)

An ordinarily skilled artisan would comprehend *user input* as a term indicating structure.

User inputs (and user selections) are disclosed in the specification of the ‘644 Patent. 5:42-49; 6:11-16; 14:16-23; Fig. 7 (IDS Console 703b); Fig. 8 (Management Console(s) 803); *see also* Figs. 9-11.

Further, *user input* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *user inputs* and *user interfaces*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-5 (US Patent No. 6,321,334, 13:47-49 (security configuration user interface); Figs. 4-9); Appendix A-6 (US Patent Application Publication No. 2002/0104014, [0039] (console; user interface); Fig. 1 (console 105)); Appendix A-7 (US Patent Application Publication No. 2002/0026591, Fig. 1 (GUI 18, Interface 14)); Appendix A-9 (US Patent Application Publication No. 2003/0014669, Abstract). Thus, *user input* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

2. Claim Terms for Updating a Firewall and an Intrusion Prevention System (Claim Terms 24-29)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “intrusion prevention system,” “firewall,” “user input,” “update,” “vulnerability,” and “network.” Two claims in this group recite the terms “system component,” which receive structural support from adjacent terms which describe structure, as well as from a view of the claims as a whole:

“firewall occurrence mitigation system component” (Claim Term 28) and “intrusion prevention system component” (Claim Term 29).

a. *intrusion prevention system* (Claim Terms 25, 27, 29)

As already argued, *intrusion prevention system* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.a., *supra*.

b. *firewall* (Claim Terms 24, 26, 28)

As already argued, *firewall* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.b., *supra*.

c. *user input* (Claim Terms 24, 25)

As already argued, *user input* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.d., *supra*.

d. *update* (Claim Terms 28, 29)

The term *update* is very closely related to *software update*. As already argued, *software update* (and therefore, *update*) is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.c., *supra*.

e. *vulnerability* (Claim Terms 26-29)

An ordinarily skilled artisan would comprehend *vulnerability* as a term indicating structure. *Vulnerabilities* are referenced and disclosed extensively in the specification of the ‘644 Patent. *See, e.g.* Abstract; 1:27-37; 2:1-3; 2:36-39; 3:8-10; 4:1-12; Fig. 5B (Anti-Vulnerability Platform; Vulnerability Management point product); Fig. 6 (Anti-Vulnerability Engine/Service, Vulnerabilities Database); Fig. 12 (Anti-Vulnerability Platform). Further, *vulnerability* is a term an ordinarily skilled artisan would have understood at the date to which

the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *vulnerabilities*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-4 (US Patent No. 6,298,445, Table 1 (Security vulnerabilities database)); Appendix A-6 (US Patent Application Publication No. 2002/0104014, [0004]); Appendix A-7 (US Patent Application Publication No. 2002/0026591, Abstract; [0008] (store of known vulnerabilities)); Appendix A-8 (US Patent Application Publication No. 2002/0199122, Abstract; Fig. 1 (Vulnerability Bulletin Sources 34)); Appendix A-9 (US Patent Application Publication No. 2003/0014669, Abstract; [0010] (vulnerability detection); [0059]). Thus, *vulnerability* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

f. *network* (Claim Terms 24, 25)

An ordinarily skilled artisan would comprehend *network* (as well as the related terms *device*, *plurality of devices*, and *networked device(s)*) as a term indicating structure. The field of the inventions of the Patents-in-Suit “relates to computer systems, and more particularly to management of security of computing and network devices that are connected to other such devices.” *See generally* ‘644 Patent. Further, *network* and the related terms *device*, *plurality of devices*, and *networked device(s)* are terms an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent,

which make reference to or disclose *network* and the related terms *device*, *plurality of devices*, and *networked device(s)*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-3 (US Patent No. 5,892,903, Abstract; 1:13-22; Fig. 1); Appendix A-4 (US Patent No. 6,298,445, Abstract; Fig. 1); Appendix A-5 (US Patent No. 6,321,334, Abstract; Fig. 2); Appendix A-9 (US Patent Application Publication No. 2003/0014669, Abstract). Thus, *network* and the related terms *device*, *plurality of devices*, and *networked device(s)* are terms “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

3. Claim Terms Concerning Identifying an Occurrence in Connection with a Device (Claim Terms 30-31)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “occurrence,” “plurality of devices,” and “networked device.”

a. *occurrence* (Claim Terms 30-31)

An ordinarily skilled artisan would comprehend *occurrence* and the related term *attack* as terms indicating structure. *Occurrences* are referenced and disclosed in the specification of the ‘644 Patent. *See, e.g.* 1:25-37; 4:41-53; Fig. 1 (Attacker 115). Further, *occurrence* and *attack* are terms an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *attacks* and closely related concepts. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-3 (US Patent No. 5,892,903,

Abstract; Fig. 2; 6:23-34); Appendix A-4 (US Patent No. 6,298,445, 1:17-26; 1:42-46; 2:18-28; Fig. 2 (external unauthorized users 8; intruder detector 48)); Appendix A-8 (US Patent Application Publication No. 2002/0199122, Fig. 2 (Damage 10; System Compromise, Denial of Service 12; Root Break-in 14, etc.)). Thus, *occurrence* and the related term *attack* are terms “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

b. plurality of devices/networked device (Claim Terms 30-31)

As already argued, the terms *plurality of devices* and *networked device* are “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.b., *supra*.

4. Claim Terms for Determining Whether Devices Are Actually Vulnerable to an Occurrence or Attack (Claim Terms 32-35)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “vulnerability,” “plurality of devices,” “occurrence,” and “attack.”

a. vulnerability (Claim Terms 32-35)

As already argued, *vulnerability* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.2.e., *supra*.

b. plurality of devices/networked device (Claim Terms 32-35)

As already argued, the terms *plurality of devices* and *networked device* are “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.b., *supra*.

c. occurrence/attack (Claim Terms 32-35)

As already argued, *occurrence* and *attack* are terms “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.a., *supra*.

5. Claim Terms Concerning Storing Information Associated with Multiple Actual Vulnerabilities (Claim Terms 36-37)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “vulnerabilities” and “data storage.”

a. *vulnerability* (Claim Terms 36-37)

As already argued, *vulnerability* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.2.e., *supra*.

b. *data storage* (Claim Terms 36-37)

An ordinarily skilled artisan would comprehend *data storage* as a term indicating structure. *Data storage* is referenced and disclosed in the specification of the ‘644 Patent. *See*, e.g. 1:66 (defining “data warehouse” as a component that contains vulnerabilities and updates for devices that operate on at least one network); 2:4-6, 21; 3:22-23; 4:8; Fig. 1 (V&R DATABASE 110); Fig. 2 (DATABASE 146, 156, 166); Fig. 5B (Data Warehouse); Fig. 6 (Vulnerabilities Database); Fig. 12 (Data Warehouse and databases). Further, *data storage* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *data storage*, *databases* and closely related concepts. Appendix A-2 (Prosecution history of ‘699 Patent,

Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-4 (US Patent No. 6,298,445, Table 1 (Security vulnerabilities database)); Appendix A-6 (US Patent Application Publication No. 2002/0104014, [0039] (databases)); Appendix A-7 (US Patent Application Publication No. 2002/0026591, Fig. 1 (Security system database 30); Fig. 5 (Vulnerability database 70)); Appendix A-9 (US Patent Application Publication No. 2003/0014669, Abstract ; [0067]). Thus, *data storage* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

6. Claim Terms Concerning Data Storage of Device and Vulnerability Information (Claim Terms 38-42)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “data storage/structure,” “attack,” “vulnerability,” “plurality of devices/networked device,” “intrusion prevention system,” “operating system,” “patch,” “policy,” and “configuration.”

a. data storage/data structure (Claim Terms 38-42)

As already argued, *data storage* (and the closely related *data structure*) is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See V.B.5.b., supra.*

b. attack (Claim Terms 38-40)

As already argued, *attack* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See V.B.3.a., supra.*

c. vulnerability (Claim Terms 38-42)

As already argued, *vulnerability* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See V.B.2.e., supra.*

d. plurality of devices/networked devices (Claim Terms 41, 42)

As already argued, the terms *plurality of devices* and *networked device* are “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.b., *supra*.

e. intrusion prevention system (Claim Term 40)

As already argued, *intrusion prevention system* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.a., *supra*.

f. operating system (Claim Term 39)

An ordinarily skilled artisan would comprehend *operating system* as a term indicating structure. An *operating system* is referenced and disclosed in the specification of the ‘644 Patent. *See, e.g.* 1:66 (defining “data warehouse” as a component that contains vulnerabilities and updates for devices that operate on at least one network); 2:4-6, 21; 3:22-23; 4:8; Fig. 1 (V&R DATABASE 110); Fig. 2 (DATABASE 146, 156, 166); Fig. 5B (Data Warehouse); Fig. 6 (Vulnerabilities Database); Fig. 12 (Data Warehouse and databases). Further, *operating system* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose an *operating system*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-3 (US Patent No. 5,892,903, 1:22-29); Appendix A-4 (US Patent No. 6,298,445, Fig. 5 (OPERATING SYSTEM 74)); Appendix A-5 (US Patent No. 6,321,334, Fig. 1 (Operating

System 135). Thus, *operating system* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

g. *patch* (Claim Term 38)

The term *patch* is very closely related to *software update*. As already argued, *software update* (and therefore, *patch*) is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.1.c., *supra*.

h. *policy* (Claim Term 38)

An ordinarily skilled artisan would comprehend *policy* as a term indicating structure. *Policy* is referenced and disclosed in the specification of the ‘644 Patent. *See, e.g.* 2:32-35; 4:41-53; 6:8-10; Fig. 10 (Security Policy Templates, Rules, & Updates). Further, *policy* is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to a patent issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which discloses *policy*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see* Appendix A-5 (US Patent No. 6,321,334, 13:47-49 (security configuration user interface); Fig. 2 (Security Configuration UI 226); Fig. 3 (Configure system security policy)). Thus, *policy* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

i. *configuration* (Claim Terms 38, 41, 42)

An ordinarily skilled artisan would comprehend *configuration* as a term indicating structure. *Configuration* is referenced and disclosed in the specification of the ‘644 Patent. *See, e.g.* 2:32-35; 2:48-59; 2:63 – 3:7. Further, *configuration* is a term an ordinarily skilled artisan

would have understood at the date to which the Patents-in-Suit claim priority. Plaintiff points to patents and patent application publications issuing contemporaneously with the priority date of the Patents-in-Suit and listed on an Information Disclosure Statement in the prosecution history of the ‘699 Patent, which make reference to or disclose *configuration*. Appendix A-2 (Prosecution history of ‘699 Patent, Information Disclosure Statement) at 82; *and see, e.g.* Appendix A-5 (US Patent No. 6,321,334, 13:47-49 (security configuration user interface); Fig. 2 (Security Configuration UI 226); Fig. 3 (Configure system security policy)); Appendix A-7 (US Patent Application Publication No. 2002/0026591, Fig. 2 (Configuration detection subsystem 38)). Thus, *configuration* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Williamson* at 1349.

7. Additional Claim Terms (Claim Terms 43-45)

Words understood by persons of skill in the art “to have a sufficiently definite meaning as the name for structure” which are common in this group of claim terms include “occurrence,” “networked device,” and “vulnerability.”

a. *occurrence* (Claim Terms 43, 45)

As already argued, *occurrence* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.a., *supra*.

b. *networked device* (Claim Terms 43-45)

As already argued, the terms *plurality of devices* and *networked device* are “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.3.b., *supra*.

c. *vulnerability* (Claim Terms 38-42)

As already argued, *vulnerability* is a term “understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *See* V.B.2.e., *supra*.

C. In the event the disputed terms are governed by 35 U.S.C. § 112(f), the specification discloses structure sufficient to be understood by one skilled in the art as adequate to perform the functions recited in the claims, rendering the claims definite.

Defendants have failed to carry the burden of rebutting the presumption against application of § 112(f) to the disputed claims. Without conceding its argument against Defendants’ § 112(f) position, Plaintiff submits that the disputed claims would nonetheless remain valid under a means-plus-function construction. Defendants assert that the specification fails to disclose sufficient structure to support the functions in the claims: “As a result, the specification fails to provide any detailed flowcharts, diagrams, or specific sets of instructions sufficient to satisfy the numerous functions recited in the claims.” D.I. 91 at 23. Plaintiff disagrees, because Defendants have failed to justify a requirement for such detail when the disclosed structure is sufficient to be understood by one skilled in the art as adequate to perform the functions recited in the claims.

Defendants rely on *Blackboard*, *Aristocrat*, and *Augme* in arguing that under § 112(f) the disputed claim limitations would be indefinite because the specification fails to provide an algorithm that performs the claims’ recited functions. *See generally* D.I. 91 at 22-30 (citing *Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371(Fed. Cir. 2009); *Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328 (Fed. Cir. 2008); *Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326 (Fed. Cir. 2014)). Defendants cannot persuade that these cases are applicable, because they fail to even argue that they can apply when the claims in question are not expressly written as mean-plus-function claims.

Blackboard, *Aristocrat*, and *Augme* all dealt with the construction of claims written in express “means for” format. *See Blackboard* at 1382; *Aristocrat* at 1333; *Augme* at 1337. But courts have declined to apply *Aristocrat* and its progeny where, as in this case, claims are not written in mean-plus-function form. Defendants have made a superficial argument in favor of construction under § 112(f), in which they ignore substantial existing authority against equating “code” with “means,” and now essentially ask the Court to do what the defendant in *eWinWin* asked: “[Defendant] is asking this Court to use the *Aristocrat* line of cases, in which MPF claim limitations were at issue and the courts were determining whether sufficient structure was disclosed, to find that MPF claim limitations exist in the [patent-in-suit] *in the first place*.¹” *eWinWin, Inc. v. Groupon, Inc.*, No. 8:10-CV-2678-T-24, 2011 WL 6012194, at *13 (M.D. Fla. Sept. 5, 2011) (emphasis added) (finding that “component” was not part of an MPF claim limitation); *see also Chamberlain* at 976–77 (finding that “code generator” claim elements connote structure to one skilled in the art, and declining to construe those elements as means-plus-function); *Atser Research Techs., Inc. v. Raba-Kistner Consultants Inc.*, No. SA-07-CA-93-H, 2009 WL 691118, at *12–14 (W.D. Tex. Mar. 2, 2009), aff'd 384 F. App'x 995 (Fed. Cir. 2010) (“While it may seem a paradox . . . the statute allows the patentee the choice to present his claim in means-plus-function format and rely on the specification for structure or to specify a particular claim that passes the patent examination in non-means form.”). *Blackboard* and *Aristocrat* are inapplicable in this case.

Moreover, the questions in *Blackboard* and *Aristocrat* are far away from the one at issue here. In *Blackboard*, the plaintiff argued that an algorithmic means-plus-function claim was not indefinite because “a person skilled in the art could readily fashion a computer based means for performing the claimed function.” *Blackboard* at *14. Plaintiff has not, in the words of the

Blackboard court, “look[ed] to the knowledge of one skilled in the art apart from and unconnected to the disclosure of the patent.” *Id.* Rather, Plaintiff’s position is that an ordinarily skilled artisan would understand that the *disclosure* of the patent encompasses software for the claimed functions and would be able to implement such a program. The vague disclosure at issue in *Aristocrat* is similarly far removed: there, the court held a claim indefinite, as the specification did not disclose sufficient structure where disclosure stated one of ordinary skill in the art could program a computer with “appropriate programming” to perform a “control means” function. *Aristocrat* at 1333-34. Plaintiff has already extensively detailed the manner in which the claims at issue and the patent specification disclose elements well understood by an ordinarily skilled artisan to represent structure. *See* V.B.1. - V.B.7., *supra*. Defendants’ reliance on *Blackboard* and *Aristocrat* is unavailing.

Defendants have failed to overcome the presumption that § 112(f) does not apply to the disputed claims. Further, Defendants cannot show, by clear and convincing evidence, that the disputed claims are indefinite if construed under § 112(f).

VI. CONCLUSION

For at least the foregoing reasons, Plaintiff respectfully asks the Court to adopt its proposed claim constructions.

Dated: January 22, 2018

Respectfully submitted,

BUETHER JOE & CARPENTER, LLC

By: /s/ Christopher M. Joe

Christopher M. Joe
State Bar No. 00787770
Chris.Joe@BJCIPLaw.com
Michael D. Ricketts
State Bar No. 24079208
Mickey.Ricketts@BJCIPLaw.com

1700 Pacific Avenue
Suite 4750
Dallas, Texas 75201
Telephone: (214) 466-1272
Facsimile: (214) 635-1828

Of Counsel:

Sean T. O'Kelly (DE No. 4349)
George Pazuniak DE (No. 478)
Daniel P. Murray (DE No. 5785)
Thomas H. Kramer (DE No. 6171)
O'Kelly & Ernst, LLC
901 N. Market Street, Suite 1000
Wilmington, Delaware 19801
(302) 778-4000
(302) 295-2873 (facsimile)
sokelly@oeblegal.com
gp@del-iplaw.com
dmurray@oeblegal.com
tkramer@oeblegal.com

Thomas F. Meagher
Alan Christopher Pattillo
Meagher Emanuel Laks Goldberg & Liao, LLP
One Palmer Square
Suite 325
Princeton, NJ 08542
(609) 454-3500
tmeagher@meagheremanuel.com
cpattillo@meagheremanuel.com

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule 5.1(d). As such, this document was served on all counsel who are registered users of ECF on this 22nd day of January, 2018.

By: /s/ Christopher M. Joe

Christopher M. Joe